# Datenschutzkonzept

# Unternehmenserklärung zum Datenschutz und Datensicherheit

Version: letzte Freigabe
Gültig ab: letzte Freigabe



OPTIMAL SYSTEMS GmbH
Unternehmenszentrale
Cicerostraße 26
10709 Berlin

# Änderungsübersicht und Freigabeinformationen

| Vers | Erstellt durch | Änderung | Erstellt am | Freigabe durch | Freigabe am |
|---|---|---|---|---|---|
| 6.0.0 | Stefan Eberle | Review, Strukturanpassung; Änderungsübersicht neues Format (alte Vers wurden bis 2.2 geführt, zur Angleichung Vers und Variante hier weiter mit 6.0.0) | 01.04.2020 | Gregor Wolf | 06.04.2020 |
| 7.0.0 | Lisa Gough/ Stefan Eberle | Kleinere Korrekturen, Benennung Stefan Eberle als externen Datenschutzbeauftragten | 19.06.2020 | Gregor Wolf | 01.07.2020 |


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

# Inhaltsverzeichnis





Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

# 1 Einleitung

## 1.1 Zweck und Geltungsbereich

Mit diesem Dokument werden

- das grundsätzliche Verständnis von Datenschutz und Datensicherheit insbesondere im Umgang mit auftragsbezogenen Kundendaten, aber auch darüber hinaus, für die OPTIMAL SYSTEMS GmbH (OS) postuliert und
- sich daraus ableitende Handlungsrichtlinien definiert.

Als Softwarehersteller und Lösungsanbieter im Bereich Enterprise Content Management ergeben sich im täglichen Betrieb des Unternehmens vielfältige Berührungspunkte mit datenschutzrelevanten Bereichen. So kommt es im Zusammenhang mit der Einführung unseres Produktes enaio® bei Kunden immer dazu, dass im Rahmen der Tätigkeit auf Kundendaten zugegriffen wird oder diese zu Analysezwecken OPTIMAL SYSTEMS zur Verfügung gestellt werden. Gleiches gilt für den Bereich der technischen Kundenbetreuung und des Supports.

Nach Artikel 28ff – Auftragsverarbeiter - der EU-Datenschutzgrundverordnung (DS-GVO) ist bei der Auftragsverarbeitung jeweils der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer bereichsspezifischer Regelungen zum Datenschutz verantwortlich. Aus diesem Grunde werden üblicherweise individuelle Datenschutzvereinbarungen zwischen OPTIMAL SYSTEMS und dem jeweiligen Auftraggeber vereinbart.

## 1.2 Gültigkeitsbereich

Dieses Dokument gilt für alle Bereiche und Mitarbeiter der OPTIMAL SYSTEMS GmbH und deren mehrheitlich beteiligter Tochterunternehmen und hat für alle Angestellten des Unternehmens verbindlichen Charakter.

## 1.3 Zuständigkeiten

### 1.3.1 OPTIMAL SYSTEMS

Review und Genehmigung dieses Dokumentes erfolgt durch den Geschäftsbereichsleiter Professional Services und den Datenschutzbeauftragten des Unternehmens.

Dieses Dokument unterliegt einem Review innerhalb von maximal 3 Jahren. Dafür ist der Datenschutzbeauftragte des Unternehmens verantwortlich.

Die OPTIMAL SYSTEMS GmbH hat einen Datenschutzbeauftragten gem. Art. 37 DSGVO i.V. m. § 38 BDSG benannt:


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

**Stefan Eberle**

von der Industrie- und Handelskammer
öffentlich bestellter und vereidigter Sachverständiger
für Telekommunikation und Verbindungspreisberechnung
sowie für Technik und Systeme der Informationsverarbeitung
Zuständige IHK: IHK Berlin

Hobeckweg 34
12623 Berlin
adv@optimal-systems.de
+4930 895 708 0

### 1.3.2 Qualitätsoperationen

Review dieses Dokumentes durch einen Qualitätsmanager

# 2 Begriffe und Definitionen

Die im vorliegenden Dokument verwendeten Begriffe orientieren sich in ihrer Verwendung an den Definitionen der DIN EN 9001:2000, Kapitel 2 und der im Artikel 4 der DS-GVO festgehaltenen Begriffsbestimmung.

# 3 Unternehmensstrategie zu Datenschutz und Datensicherheit

Die Unternehmensstrategie wurde durch die Geschäftsführung der OPTIMAL SYSTEMS GmbH wie folgt definiert:

1. Das Tätigkeitsfeld der OPTIMAL SYSTEMS GmbH bedingt hohe Anforderungen an Datenschutz und Datensicherheit. Im Rahmen der Kundenbeziehungen erhält die OPTIMAL SYSTEMS tiefe Einblicke in die Unternehmensprozesse und die damit verbundenen Daten ihrer Kunden. Darüber hinaus kommt es zum Zugriff auf schützenswerte Daten Dritter, z.B. Patientendaten in einem Krankenhaus.

   **Aus diesem Grunde stellt der Datenschutz und die Datensicherheit eines der wichtigsten Qualitätsziele des Unternehmens dar und ist in das Qualitätsmanagementsystem integriert.**

2. Datenschutz und Datensicherheit umfassen bei OPTIMAL SYSTEMS
   - den Schutz personenbezogener Daten gemäß den gesetzlichen Vorschriften der DSGVO, des BDSG und anderer Vorschriften über den Datenschutz,
   - die Sicherheit bei der Verarbeitung vertraulicher Personen- und Betriebsdaten des Kunden,
   - die Gewährleistung des störungsfreien Betriebs der Informationstechnik (IT-Sicherheit) als Voraussetzung für eine sichere Verarbeitung.

3. Datenschutz und Datensicherheit sind in das Management des Unternehmens integriert. Die Führungskräfte der Unternehmensbereiche tragen die persönliche Verantwortung für die Durchsetzung der dazu getroffenen Festlegungen.

4. Die konkreten Maßnahmen und die Verantwortlichkeiten sind detailliert in firmeninternen Verfahrens- und Arbeitsanweisungen festgelegt und werden im Rahmen des Qualitätsmanagementsystems der Firma sowohl extern als auch intern auditiert und bewertet.

5. Der Beauftragte für den Datenschutz wirkt auf die Einhaltung der DS-GVO, des Bundesdatenschutzgesetzes sowie anderer Vorschriften über den Datenschutz hin. Durch die Einflussnahme auf die Gestaltung der innerbetrieblichen Organisation im Sinne des Artikel 25 ff. DS-GVO und – soweit anwendbar - § 64 BDSG (Anforderungen an die Sicherheit der Datenverarbeitung) unterstützt er den IT-Sicherheitsprozess und die Datensicherheit insgesamt.

6. Die Mitarbeiter des Unternehmens werden durch die persönliche, vertragliche Verpflichtung auf das Datengeheimnis sowie durch angemessene Schulungen und periodische Unterweisungen motiviert und befähigt, die vorgegebenen Festlegungen zu Datenschutz und Datensicherheit an ihrem Arbeitsplatz zuverlässig und ordnungsgemäß einzuhalten.


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

# 4 Organisation von Datenschutz und Datensicherheit

## 4.1 Definition von Schutzstufen

Ausgehend von der Datenschutzstrategie und dem individuellen Schutzbedarf von Kundendaten sind für die Unternehmensbereiche der OPTIMAL SYSTEMS folgende Schutzstufen festgelegt:

- ein Grundschutz, der für alle Unternehmensbereiche und Geschäftsstellen der Firma verbindlich ist
- und ein erweiterter Datenschutz, der je nach den individuellen Erfordernissen der einzelnen Unternehmensbereiche und der jeweiligen Kundenbeziehung einzuhalten ist.

## 4.2 Grundschutz

Der durch OPTIMAL SYSTEMS gewährleistete allgemein verbindliche Grunddatenschutz umfasst folgende Maßnahmen:

- die Durchsetzung, der auf der Grundlage der DS-GVO und des BDSG festgelegten Maßnahmen des Schutzes personenbezogener Daten,
- die technischen und organisatorischen Maßnahmen der Datensicherung gem. Artikel 28ff DS-GVO und – soweit anwendbar - § 64 BDSG, die auch bei der Auftragsverarbeitung vertraulicher Personen- und Betriebsdaten anzuwenden sind,
- die für die konkreten Betriebsbedingungen zutreffenden Verfahren der IT-Sicherheit.

## 4.3 Erweiterter Datenschutz

Die erweiterten Datenschutzmaßnahmen werden durch die jeweils zuständigen Geschäftsbereichsleiter in enger Zusammenarbeit mit den Kunden und dem Datenschutzbeauftragten festgelegt.

Dabei wird u. a. folgendes berücksichtigt:

- Gegenstand und Ziele der speziellen Festlegungen,
- einzuleitende zusätzliche Schutzmaßnahmen, die über die Festlegungen für den Grunddatenschutz hinausgehen,
- der zusätzliche finanzielle, personelle und technische Aufwand und dessen Realisierung,
- Zuständigkeiten und Verantwortung für die Einführung und Kontrolle.

Die mit den Kunden individuell vereinbarten Datenschutzvereinbarungen werden den davon betroffenen Mitarbeitern des Unternehmens nachweislich zur Kenntnis gebracht.


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

## 4.4 Kontrolle und Bewertung

Durch die in allen Unternehmensbereichen vom Datenschutzbeauftragten und dem Qualitätsmanager durchgeführten internen Audits und deren Bewertung durch die Geschäftsführung, wird eine permanente Weiterentwicklung des Datenschutzsystems gewährleistet.

# 5 Maßnahmen zu Datenschutz und Datensicherheit

## 5.1 Maßnahmen des Datenschutzes nach DS-GVO und BDSG

### 5.1.1 Beauftragter für den Datenschutz

Die OPTIMAL SYSTEMS GmbH hat gemäß Artikel 37 DS-GVO bzw. § 38 BDSG einen Beauftragten für den Datenschutz bestellt. Dieser ist der Geschäftsführung berichtspflichtig, führt in dessen Auftrag periodisch und zu speziellen Sicherheitsmaßnahmen Kontrollen und Audits durch und unterbreitet Vorschläge zur kontinuierlichen Vervollkommnung von Datenschutz und Datensicherheit im Unternehmen.

Schwerpunkt seiner Tätigkeit ist neben der Gewährleistung des Schutzes personengebundener Daten der Mitarbeiter die Sicherheit der nach Artikel 28 DS-GVO und - soweit anwendbar - § 62 BDSG im Auftrag zu verarbeitenden Kundendaten.

Dabei arbeitet er eng mit den für die Verarbeitung der Daten verantwortlichen Geschäftsbereichsleitern zusammen und nimmt Einfluss auf die Einbeziehung der Datenschutzmaßnahmen in die Arbeitsprozesse des Unternehmens.

### 5.1.2 Verpflichtungen

Alle Mitarbeiter der OPTIMAL SYSTEMS GmbH werden in ihrem Arbeitsvertrag neben ihrer Verschwiegenheitspflicht unterschriftlich auf das Datengeheimnis nach Artikel 28 Abs. 3b) DS-GVO und – soweit anwendbar - § 53 BDSG verpflichtet und darüber belehrt, dass Verstöße dagegen ggf. nach Artikel 82 und 83 der DS-GVO und §§ 41 bis 43 BDSG und anderen einschlägigen Rechtsvorschriften geahndet werden und mit arbeitsrechtlichen Maßnahmen verbunden sein können.

Darüber hinaus erfolgt üblicherweise auf Wunsch von Kunden aus bestimmten Branchen bei der Verarbeitung besonders sensibler Kundendaten oder bei besonderen Verarbeitungsbedingungen, z.B. ein Direktzugriff auf produktive IT-Systeme der Kunden, eine spezielle Verpflichtung der betreffenden Mitarbeiter nach einem vorgegebenen Verpflichtungstext des Kunden.


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

### 5.1.3 Unterweisungen

OPTIMAL SYSTEMS führt periodisch (in der Regel jährlich) oder zu besonderen Anlässen Datenschutzunterweisungen durch, mit dem Ziel, ihre Führungskräfte und alle Mitarbeiter für die Durchsetzung des Datenschutzes zu sensibilisieren und zu motivieren, ihr Verständnis und ihre Unterstützung für die festgelegten Maßnahmen zu erreichen sowie sie zu befähigen, die festgelegten Sicherheitsmaßnahmen korrekt und sinnvoll anzuwenden.

Darüber hinaus besteht auf Kundenwunsch die Möglichkeit, zu bestimmten Anwendungen der Auftragsverarbeitung neben der allgemeinen Einweisung, spezielle Unterweisungen zu Fragen des Datenschutzes durchzuführen.

### 5.1.4 Kontrollen und Audits

Durch die vom Datenschutzbeauftragten und dem Qualitätsmanager jährlich durchgeführten internen Audits und deren Bewertung durch die Geschäftsführung wird eine permanente Weiterentwicklung des Datenschutzsystems gewährleistet. Davon unberührt bleibt die Verpflichtung aller Führungsebenen des Unternehmens mindestens quartalsweise die Einhaltung der Datenschutzbestimmung für ihren Zuständigkeitsbereich zu kontrollieren.

Auf Wunsch von Kunden besteht nach vorheriger Abstimmung die Möglichkeit, die Ordnungsmäßigkeit der Auftragsverarbeitung ihrer Daten in den Betriebstätten des Unternehmens persönlich zu kontrollieren.

## 5.2 Technische und organisatorische Maßnahmen

Die wirksame und gesetzeskonforme Organisation des Datenschutzes hat bei OPTIMAL SYSTEMS eine lange Tradition. In diesem Sinne wurden die technischen und organisatorischen Maßnahmen am Anforderungskatalog / Schichtenmodell gemäß Anlage zum § 11 des bis zum 27.05.2018 gültigen Bundesdatenschutzgesetzes (BDSG alt) ausgerichtet. Aufgrund der Fortführung bzw. Weiterentwicklung dieser Kategorisierung im § 64 des derzeit gütigen Bundesdatenschutzgesetzes (BDSG neu) wird die herkömmliche Gliederung innerhalb der neu vorgegeben Struktur beibehalten. Darüber hinaus gehende Anforderungen des § 64 BDSG (neu) werden als zusätzliche Anforderung gemäß Kapitel 4.3 dieses Dokuments gewertet und dementsprechend auftragsbezogen separat dokumentiert. Dieser Paragraf ist ausschließlich für ausgewählte öffentliche Auftraggeber anwendbar. Eine grundsätzliche Implementierung bzw. Dokumentation des hier geforderten Maßnahmenumfanges wird für andere Kunden als nicht praktikabel angesehen.

Die nachfolgende Klassifizierung der technischen und organisatorischen Maßnahmen erfolgt anhand der Gliederung des Artikel 32 DS-GVO. Die genaue technische Umsetzung der benannten Maßnahmen ist in der Anlage „Technische und organisatorische Maßnahmen (TOM) zum Datenschutzkonzept“ in der aktuellen Version beschrieben.


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

Elektronisch vorliegende Kundendaten sind verpflichtend im firmeneigenen ECM-System abzulegen und unterliegen somit automatisch den erweiterten Sicherheits- und Schutzmechanismen von enaio®.

### 5.2.1 Gewährleistung der Vertraulichkeit

Die Vertraulichkeit personenbezogener Daten ist gemäß Artikel 5 DS-GVO eine grundsätzliche Forderung für die Verarbeitung personenbezogener Daten. Sie umfasst den Schutz dieser Daten vor unbefugter oder unrechtmäßiger Verarbeitung insgesamt.

Somit beinhaltet der Bereich Vertraulichkeit alle Maßnahmen

- der Zutrittsbeschränkung zu Räumlichkeiten, in den eine Verarbeitung vorgenommen wird (Zutrittskontrolle),
- der Zugangskontrolle zu den Verarbeitungssystemen,
- der Zugriffskontrolle zu den Verarbeitungsprogrammen und -daten auf bzw. in diesen Verarbeitungssystemen sowie
- der vereinbarungsgemäßen (Auftragskontrolle) und
- zweckgebundenen Durchführung der Verarbeitungsvorgänge (Trennungskontrolle).

### 5.2.2 Gewährleistung der Integrität

Die Integrität der personenbezogenen Daten wird als Grundsatz der Verarbeitung im Artikel 5 DS-GVO festgelegt. Sie beinhaltet den Schutz dieser Daten vor unbeabsichtigtem Verlust und unbeabsichtigter Zerstörung.

Die technischen und organisatorischen Maßnahmen umfassen alle Aspekte

- der Weitergabe und des Transports personenbezogener Daten (Weitergabekontrolle) und
- der Nachvollziehbarkeit und Dokumentation der Datenverwaltung und Pflege (Eingabekontrolle).

### 5.2.3 Gewährleistung der Verfügbarkeit und Belastbarkeit

Es wird gewährleistet, dass personenbezogene Daten vor zufälliger Zerstörung oder Verlust geschützt sind. Dafür sind folgende Maßnahmen vorgesehen:

- die allgemeinen Maßnahmen zum Schutz vor zufälliger Zerstörung oder Verlust durch Wasserschäden, Blitzschlag oder Stromausfall,
- die Aufstellung von Feuerlöschgeräten in allen Räumen, in denen Daten verarbeitet oder gelagert werden,


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

- die Stabilisierung der Verarbeitungssysteme mit Geräten der unterbrechungsfreien Spannungsversorgung (USV),
- die Erstellung von Sicherheitskopien und Protokollieren von Dateiänderungen
- der Einsatz von Management- und Überwachungssystemen zur Sicherstellung eines ordnungsgemäßen Betriebs des firmeneigenen Netzwerks und der angeschlossenen Datenverarbeitungsanlagen
- die Definition von Meldewegen und Notfallplänen im Störungsfall

### 5.2.4 Regelmäßige Überprüfung, Bewertung und Evaluierung

Grundsätzlich erfolgt eine regelmäßige Überprüfung, Bewertung und Evaluierung der technischen und organisatorischen Maßnahmen durch interne Kontrollen und Audits gemäß Kapitel 5.1.4. Sie werden zusätzlich durch ihre praktische Anwendung in den täglichen betrieblichen Abläufen kontinuierlich überprüft. Ein sich ergebener Anpassungsbedarf wird durch die Mitarbeiter an die Vorgesetzten oder aber direkt an den Datenschutzbeauftragten gemeldet und evaluiert.

Abstimmungen mit Kunden bzw. Unterauftragnehmern über die vertragliche Gestaltung von Vereinbarungen zur Auftragsverarbeitung bzw. Anfragen von Dritten zur Herkunft von oder zum Umgang mit personenbezogenen Daten werden regelmäßig hinsichtlich einer eventuell notwendigen Anpassung der Verfahrensabläufe oder der technischen und organisatorischen Maßnahmen überprüft.

Weiterhin werden die Veröffentlichungen der Aufsichtsbehörden für Datenschutz bzw. des BSI regelmäßig zur Weiterentwicklung der Schutzmaßnahmen genutzt.

## 5.3 Maßnahmen zur Sicherheit der Informationstechnik

Die Gewährleistung einer weitreichenden IT-Sicherheit ist Grundlage für eine Durchsetzung der Ziele zum Datenschutz und zur Datensicherheit.

Für eine ausreichende und angemessene IT-Sicherheit sind in der Firma nachfolgende Maßnahmen wirksam.

### 5.3.1 IT-Grundschutz

Bei der Organisation der IT-Sicherheit orientiert sich OPTIMAL SYSTEMS am vom Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegebenen IT-Grundschutz-Katalog.

Die vom BSI gegebenen Empfehlungen für die technischen, organisatorischen, personellen und baulich-infrastrukturellen Standardsicherheitsmaßnahmen zum IT-Grundschutz werden im Unternehmen beachtet, was entscheidend zur Gewährleistung der Verfügbarkeit der IT-Systeme sowie der Wahrung von Vertraulichkeit, Integrität (Korrektheit) und Authentizität (digitale Identität) der Daten beiträgt.


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de

### 5.3.2 Einsatz des unternehmenseignen ECM-Systems

OPTIMAL SYSTEMS setzt sein eigenes Produkt enaio® als zentrales Werkzeug für die Datenverarbeitung und Datenspeicherung ein. Der Zugriff auf dieses System ist sowohl für die Unternehmenszentrale als auch für die angeschlossenen Tochterunternehmen realisiert. Innerhalb des ECM-Systems wird über ein mehrstufiges Berechtigungssystem und die Durchsetzung einer Mandantentrennung gewährleistet, dass nur berechtigte Mitarbeiter auf die für ihre jeweilige Tätigkeit notwendigen Daten zugreifen können.

# 6 Sicherheitsgarantie für die Kundendaten

Aus der Unternehmenserklärung ist ersichtlich, dass die OPTIMAL SYSTEMS GmbH entsprechend ihrer Unternehmensstrategie über ein umfangreiches und wirkungsvolles System von Maßnahmen zur Gewährleistung von Datenschutz und Datensicherheit verfügt.

Die Geschäftsführung und die Mitarbeiter garantieren ein hohes Maß an Sicherheit für die von ihren Kunden zur Auftragsverarbeitung übergebenen Dokumente und Daten.


Cicerostraße 26 · 10709 Berlin
Tel.: +49 30 895708-0 · Fax: +49 30 895708-888
E-Mail: kontakt@optimal-systems.de
Internet: www.optimal-systems.de